# 소프트웨어 관리: 필수적 보안, 사업 기회

BSA
세계 소프트웨어 조사 보고서
2018 년 6 월

# 목차

# 서론

전 세계적으로 소프트웨어는 사업체들이 매출 추적, 장부 유지, 목표 시장 설정, 고객과의 대화, 협력업체와의 협업에서부터 생산성 제고에 이르기까지 대부분의 과업을 수행하는 데 이용하는 가장 보편적이며 핵심적인 도구 가운데 하나가 되었다. 소프트웨어의 역량이 획기적으로 진보함에 따라, 이를 사업 수행 방식의 개선, 이익의 증대, 신규 시장 개척, 경쟁우위 확보의 촉매로 활용하는 조직들이 더욱 늘어가고 있다.

하지만 혁신적인 기술을 활용하려는 노력이 악성코드로의 노출을 포함하여 심각한 보안 위협에 의해 저해되는 경우가 너무 많다. 악성코드 감염이 불법 소프트웨어 사용과 밀접하게 관련되어 있음은 더욱 명확해지고 있다. 결과적으로 많은 CIO들이 불법 소프트웨어의 실질적 비용을 이해하게 되어 소프트웨어 관리를 개선하기 위한 실용적인 절차를 취하고 있다.

이러한 영향과 기회를 더 잘 이해하기 위해 IDC와 협력하여 실시한 BSA의 글로벌 소프트웨어 조사는 전 세계 110개 이상의 국가와 지역 경제에 걸쳐 개인용 컴퓨터에 설치된 불법 소프트웨어의 양과 가치의 계량화에 착수하였다. 결과에 따르면 CIO들은 불법 소프트웨어로 인해 보안 위험이 생긴다는 것을 알고 있지만 아직도 개인용 컴퓨터에 설치된 소프트웨어의 37%가 불법이다.

## 주요 추세 및 확인사항

- 불법 소프트웨어의 사용률이 약간 낮아졌지만 여전히 만연하고 있다.
- CIO들은 불법 소프트웨어가 점차적으로 위험해지고 값비싼 손실을 야기한다는 사실을 인지해가고 있다.
- 소프트웨어 규정의 준수를 개선하는 것이 현재 경제적 성장의 요인이며 보안적 의무이다.
- 조직들은 오늘날 소프트웨어 관리를 개선하고 주요 이득을 얻을 수 있는 의미있는 조치를 취할 수 있다.

따라서 이 보고서는 사이버 보안 위험이 고양된 이 시대에 조직들이 자신들의 네트워크에 있는 소프트웨어를 평가하고 불법 소프트웨어를 제거하는 중요한 첫발을 내디뎌야 한다는 점을 명확히 한다.이렇게 함으로써 유해한 사이버 공격의 위험을 줄이고 손익을 개선할 수 있다.

*불법 소프트웨어 사용에 대한 심도 깊은 분석은 소프트웨어 관리를 개선하는 강력한 대책을 실행하는 업체들이 오늘날 보안상의 위험을 줄이고 이익을 증대시키며 업체의 영업 중단 시간을 줄이고 기회를 늘릴 수 있는 효과적인 새로운 수단을 보유하고 있음을 보여준다.*

# 주요 확인사항

**불법 소프트웨어의 사용은 소폭 감소하기는 했으나 아직 만연하다.** 지난 2년간 세계적으로 불법 소프트웨어 설치 비율은 2% 줄어들었지만, 불법 소프트웨어의 사용은 전 세계적으로 경각심을 일으킬 수준이며 이는 개인용 컴퓨터에 설치된 소프트웨어의 37%에 달한다. 불법 소프트웨어의 전반적 상업적 가치도 줄어들고 있지만 조사 대상 국가의 대다수에서 이는 50% 이상을 차지하고 있다. 이러한 높은 비율은 기술 활용의 진전으로 인한 지역 경제의 혜택을 지연시키고 있음은 물론 회사의 손익을 저해하며 유례없는 보안 위험을 유발한다.

**CIO들은 불법 소프트웨어의 위험과 비용이 증가하고 있음을 인지하고 있다.** 조직들이 불법 소프트웨어 패키지를 획득 혹은 설치하거나 불법 소프트웨어가 설치된 컴퓨터를 구매할 때 악성코드를 접하게 될 가능성은 3분의 1이다. 각각의 악성코드 공격은 평균적으로 회사에 240만 달러의 비용을 유발하며 해결 시까지 최대 50일이 걸릴 수 있다. 감염으로 업체의 운영이 중단되거나 사업 데이터를 유실하게 되는 경우에는 회사의 브랜드와 명성에도 심각한 영향을 미치게 된다. 불법 소프트웨어와 관련된 악성코드에 대처하기 위한 비용도 증가하고 있다. 이제 감염된 컴퓨터 한 대당 1만 달러 이상의 비용이 들며 전 세계적으로 1년에 거의 3,590억 달러의 비용이 든다. 악성코드로 인한 보안 위협을 피하려는 것이 이제 CIO들이 회사 네트워크의 소프트웨어를 완전히 정품화하려는 첫 번째 이유이다.

**소프트웨어 규정 준수의 개선은 이제 경제적 성장의 요인이며 보안에 필수적이다.** 악성코드로 인해 증가되는 손실 때문에 사업체의 리더들은 악성코드의 침입, 데이타 침해, 그리고 기타 보안 위험에서의 주된 보호 수단으로서 최신 업데이트를 설치할 수 있는 정품 소프트웨어에 점차적으로 의존하고 있다. 점점 더 많은 지도자들이 전체 조직의 소프트웨어 관리 능력을 개선시키는 것이 사업체의 운영 중단 시간을 줄이고 현저히 이익을 증대시키는 효과적인 새로운 수단이 될 수 있다는 것을 깨닫고 있다. 실제로 IDC는 업체들이 소프트웨어 관리력을 개선시키는 실용적인 조치를 취할 때 이익을 11%까지 증대시킬 수 있다고 추정한다.

**오늘날 사업체들은 소프트웨어의 관리를 개선하고 중대한 이득을 얻기 위해 의미있는 조치를 취할 수 있다.** 이러한 이점들을 활용하기 위해 조직들은 소프트웨어 자산 관리를 개선할 수 있고 또한 그들의 기술에서 더 많은 효과를 확보할 수 있는 입증된 소프트웨어 자산 관리(SAM) 우수 사례들을 시행할 수 있다. SAM은 단지 최고 정보경영자들이 그들의 네트워크에서의 합법적이고 완전히 인가된 소프트웨어의 사용 뿐 아니라 위협적인 사이버 위험을 줄이고 생산성을 증대시키며 운영 중단 시간을 감소시키고 면허 관리를 집중화시키며 비용을 줄일 수 있도록 도움을 준다. 연구에 따르면 사업체들이 효과적인 SAM과 소프트웨어 면허 최적화 프로그램을 실행함으로써 연간 소프트웨어 비용을 30%까지 절약할 수 있었다. [1]

# 악성코드는 점차적으로 퍼지고 있고 손해를 끼치며 조직을 약화시키고 있다.

전세계적으로, 소비자들, 기업체들 그리고 국가들은 점차적으로 새로운 기술의 힘과 잠재성을 활용하기 위한 노력들이 악성코드로 초래된 심각한 잠재적 위협으로 방해받고 있다는 것을 점차 알아가고 있다. 이러한 악성코드의 위협은 이제 매일 초단위로 나타나는 8가지의 새로운 위협들과 사상 최고치를 나타낸다.그들의 출현 빈도가 증가하면서 영향력 역시 증대하고 있다.[2] 그들은 점차적으로 조직에 손실을 끼치고 조직을 약화시키고 있다.

악성코드 공격의 수는 계속 수치와 정교함에 있어서 기하급수적으로 발전하고 있다.[3] 그 예로서 2016년에 천만 개 이상의 ID를 노출시킨 15번의 데이타 침해가 있었으며 이는 2013년의 수치의 거의 두 배에 달한다.[4] 이 공격은 단지 큰 기업체들에게만 집중되는 것이 아니라, 소비자들과 모든 규모의 업체들에게도 발생한다. 실제로 2015년 전세계에 발생한 사이버 공격의 43%는 250명 미만의 소규모 업체에서 발생했다.[5] 그리고 사이버범죄자들은 이제 휴대폰 네트워크도 대상으로 삼고 있다. 휴대폰 장치에 발생하는 악성코드 변이형은 작년에 54% 가 증가하였고 매일 24,000개의 악성 휴대폰 앱들이 차단되었다.[6]

이러한 공격들은 또한 점차적으로 많은 손실을 끼치고 있다. 평균적으로 악성코드 공격은 업체에 240만불의 손실을 끼친다.[7] 각 감염은 대가 비용이 높은 업체의 가동 중단, 생산성 상실, 사업 기회의 상실 그리고 이러한 공격을 완화하기 위한 추가 정보기술 노동력의 비용을 초래할 수 있다. 이 감염이 업체의 가동 중지나 사업 데이터 손실을 초래하는 경우, 이는 사업의 명성과 브랜드에 심각하게 영향을 미칠 수 있다. 설상가상으로 이러한 감염이 미치는 경제적 손실 비용은 2014년 이후 20%까지 계속 늘고 있다. 악성코드 관련 활동은 이제 전세계 경제에 놀랍게도 매년 6천억 달러의 손실을 끼치고 있고 이는 전세계 총생산(GDP)의 0.8%에 해당한다.[8]

문제를 더 어렵게 만드는 것은 이러한 공격들은 종종 탐지하고 해결하기가 어렵다는 것이다. 조직이 악성코드 공격을 탐지하는 [9] 데는 보통 243일이 소요되고 해결하기까지 최대 50일이 걸린다.[10]

*(5페이지에서 계속)*

***악성코드의 위협은 현재 최고조에 달해 매일 매초마다 8가지의 새로운 위협이 등장하고 있다.***

# 악성코드의 영향

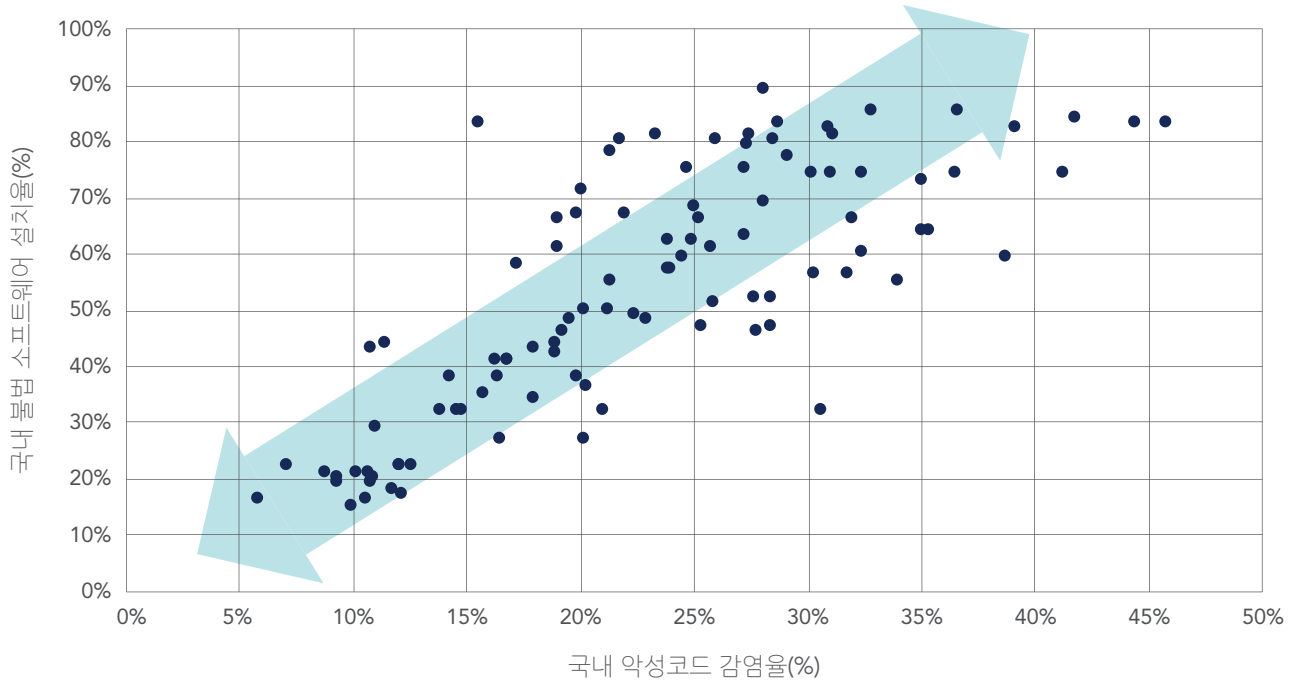
조직들은 현재 불법 소프트웨어를 획득하거나 설치할 때 거의 세 번에 한 번 꼴로 악성코드를 접하게 된다.

불법 소프트웨어와 관련된 악성코드를 다루는 것은 감염된 컴퓨터 당 1만 달러 이상 경비가 소요되며 이는 전 세계적으로 총 3,590억 달러의 경비를 의미한다.

사용자들은 다음의 사실에 주목하고 있다: 68%의 컴퓨터 사용자들과 48%의 CIO들이 불법 소프트웨어를 쓰지 않아야 할 중요한 세 가지 이유 중 하나로 평가하고 있다.

이러한 불법 악성코드 위협에 대한 CIO들의 최대 우려는 업체 혹은 개인의 데이터 손실, 시스템 중지, 네트워크의 장애 그리고 감염된 시스템을 처리하는 비용이다.

이러한 영향을 완화하기 위해서 합법 소프트웨어 사용에 관한 공식 서면 정책을 수립한 CIO의 수는 2015년 41%에서 올해 54%로 크게 증가했다. 그러나 단지 35%의 작업자들만이 공식 서면 정책을 인지하고 있으며 이는 심각한 교육적 격차를 보여준다.

적극적인 조치를 취하는 조직들은 소프트웨어 규정 준수율의 20% 상승이 업체의 수익을 11% 증진시키고 이는 조사에 참여한 평균 규모의 업체에서 50만 달러 이상의 수익 증진을 의미한다.

Source: IDC

## 악성코드 감염은 불법 소프트웨어와 연관이 있다

악성코드 감염이 불법 소프트웨어의 사용과 밀접하게 연관되어 있다는 사실, 즉 불법 소프트웨어의 사용 빈도가 높아질수록 조직을 약화시키는 악성코드 감염의 가능성이 높아진다는 것은 점차적으로 명확해지고 있다.

그럼에도 불구하고 불법 소프트웨어는 놀라운 속도로 계속 증가하고 있다. 전세계적으로 사용되는 막대한 양의 소프트웨어가 불법이다. 실제로6개 지역 중 4개 지역인 - 아시아 태평양, 중동부 유럽, 중동과 아프리카 그리고 라틴 아메리카에서 사용되는 대부분의 개인 컴퓨터의 소프트웨어가 불법이다. (12-13 페이지 참고).

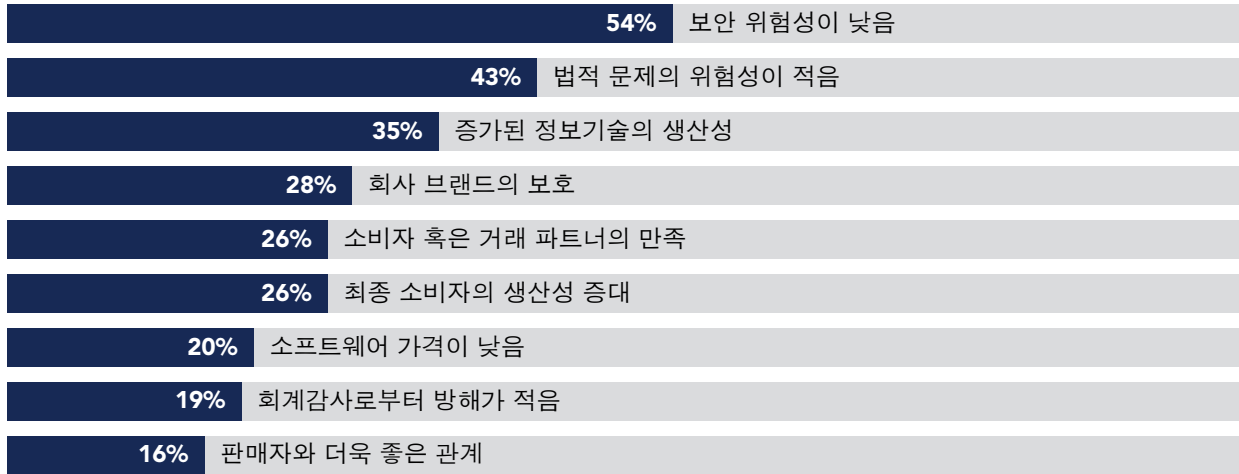
불법 소프트웨어와 악성코드의 관련성을 고려 시 이는 상당한 사이버 위험을 자아내고 있다. IDC의 평가에 의하면 불법 소프트웨어 패키지를 구하거나 설치 혹은 불법 소프트웨어가 설치된 컴퓨터를 구매하는 조직들은 1/3의 확률로 (29%) 악성코드를 접할 가능성이 있다.

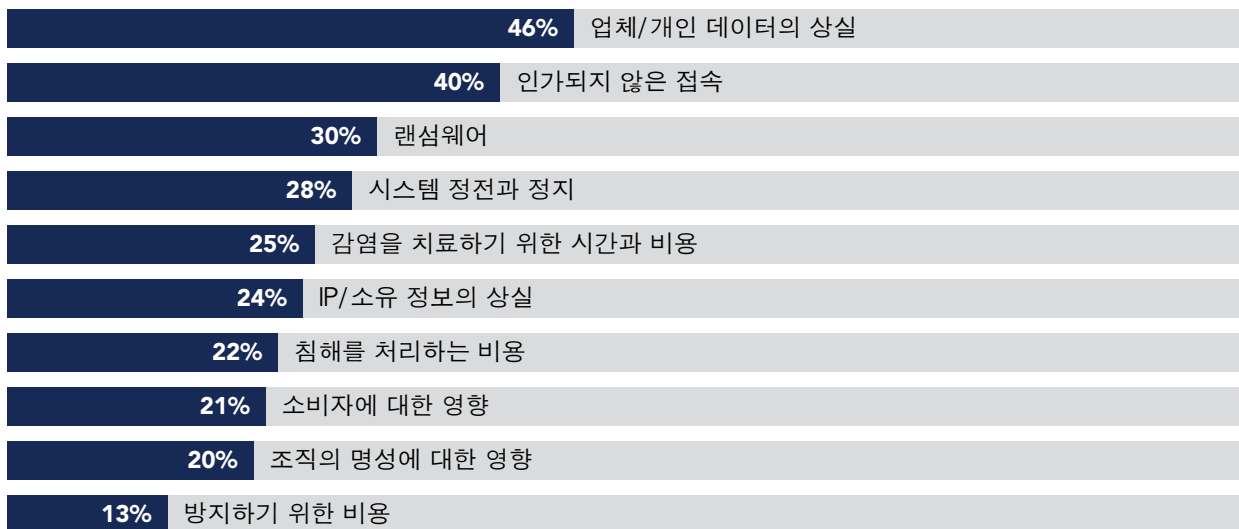
통계 분석은 이러한 연계성을 확인해주고 있다. 전세계적으로 불법 소프트웨어의 사용과 악성코드의 전염은 강력하고 일관적인 상관관계를 (r-0.78) 보여준다. 사실상 한 국가의 불법 소프트웨어 비율은 그 나라의 악성코드 전염률을 알려주는 신뢰할 만한 지표다.

CIO들은 이러한 연관성을 이해한다. 효율적인 소프트웨어 면허의 관리와 더욱 효과적인 소프트웨어 규정 준수의 주된 이점에 대해 질의하였을 때 54%의 CIO들은 소프트웨어가 모두 면허 등록이 되었는지를 확인하는 주된 이유로 보안 위험을 줄이기 위해서를 거론하였다.

CIO들은 직접 경험을 통해 악성코드 전염의 심각한 결과를 알기에 불법 소프트웨어와 악성코드의 연관성은 당연히 CIO들의 최고 주된 관심사이다. 설문에 참여한 CIO들에게 있어 불법 소프트웨어를 수반할 수 있는 악성코드에 관한 그들의 주된 관심사는 데이터의 도용이다(46%). 그들은 또한 네트워크로의 인가되지 않은 접속(40%), 잠재적 랜섬웨어에 대한 대응 (30%), 시스템 정전과 정지(28%) 그리고 네트워크를 감염으로부터 복구시키는 시간과 비용 (25%)에 대하여 주된 우려를 보고했다. 그리고

CIO들은 엄격한 소프트웨어 규정 준수에서 오는 최고의 혜택을 알린다

| 비율 | 혜택 |
| --- | --- |
| 54% | 보안 위험성이 낮음 |
| 43% | 법적 문제의 위험성이 적음 |
| 35% | 증가된 정보기술의 생산성 |
| 28% | 회사 브랜드의 보호 |
| 26% | 소비자 혹은 거래 파트너의 만족 |
| 26% | 최종 소비자의 생산성 증대 |
| 20% | 소프트웨어 가격이 낮음 |
| 19% | 회계감사로부터 방해가 적음 |
| 16% | 판매자와 더욱 좋은 관계 |

그들은 이러한 문제들이 일회성이 아님을 인지하고 있다. 실제로 설문조사에 응한 다섯 업체중 한 군데 업체는(19%) 몇 개월에 한번 이상 네트워크, 웹사이트 또는 컴퓨터의 침해를 경험하고  보안 관련 침해의 가장 흔한 원인이 최종 사용자 컴퓨터에서 발생한 악성코드로 인한 것임을(56%), 즉 불법 소프트웨어가 주된 공격의 원인인 것으로 보고하였다.

그리고 위에서 언급되었듯이 이러한 영향은 엄청난 타격을 줄 수 있다. 사이버 공격 그리고 그 결과를 처리하는 것은 이제 감염된 컴퓨터마다 1만 달러 이상의 손실을 업체에 끼치고 있으며 이는 인가된 소프트웨어를 구매하는 것보다 더 큰 비용을 업체에 치르게 만들고 이는 컴퓨터 가격보다도 훨씬 더 높은 비용이다. IDC는 불법 소프트웨어와 관련된 악성코드를 처리하는 것이 업체들에게 1년에 3,600억 달러의 비용을 초래한다고 평가하고 있다.

## 악성코드의 위험은 중대한 실질적 문제로 발전할 수 있다.

소프트웨어 자산 관리력의 상실 그리고 불법 소프트웨어로의 의존은 세계적으로 엄청난 보안 관련 파장을 일으키며 특히 불법 소프트웨어를 많이 사용하는 국가들에서 파장을 일으키고 있다. 그 예로서:

- 66%의 엄청난 양의 소프트웨어가 불법인 **중국**에서는 기하급수적으로 파장을 일으키는 악성코드로 인해 40,000개의 기관들이 장애를 경험하게 되었다. 단 하나의 악성코드가 치료되지 않은 불법 소프트웨어를 통해 빠르게 퍼져나가 Tsinghua 대학과 같은 유명 연구소들에 시스템 장애를 일으키고 전국에 걸쳐 PetroChina 주유소의 전자 지불 시스템을 정지시켰고 Bank of China의 현금 지급기를 차단시키고 China Telecom과 Hainan Airlines와 같은 유명한 업체들의 운영에도 영향을 미쳤다. 핀란드의 사이버 보안 업체인 F-Secure의 보고에 따르면 불법 소프트웨어를 사용하는 중국의 많은 컴퓨터들이 파괴적인 공격에 광범위하고 깊이 있게 영향을 미쳤다.[11] 베이징에 위치한 기술 제공업체의 한 수석 네트워크 엔지니어는 "중국 내 피해자의 대부분은 불법 사용자들이다."라고 지적하였다.[12]
- 불법 소프트웨어 사용률이 62%에 달하는 **러시아는** 12억 달러의 상업적 가치를 갖고 있으며 또한 최근 악성코드 공격으로 그 파괴적인 충격을 경험했다. 2017년에 악성코드 공격으로 러시아 보건부, 국영 러시아 철도 관리부, 경찰 병력을 관리하는 내무부 그리고 통신회사 Megafon가 시스템 장애를 겪게 되었다. 프라하 국제 관계 연구소의 한 선임 연구원은 러시아의 악성코드 감염 범위가 넓은 것은 "기한이 오래 지난 소프트웨어를 사용했을 뿐 아니라 오래된 해적판 소프트웨어"를 사용한 데서 비롯되었다고 말한다.[13]

이러한 위협의 범위와 영향은 핵심 사업 기능을 불법 소프트웨어에 의존하거나, 소프트웨어 자산 관리 시스템이 없거나, 불법 악성코드의 위험에 노출된 업체에 의존하는 이들에게 경종을 울려야 한다.

*소프트웨어 규정의 준수는 이제 경제적 성장의 요인이 되었고 보안적 의무가 되었다.*

# 소프트웨어 자산 관리로 이러한 사이버 위험을 줄이고 손익을 개선할 수 있다.

모든 소프트웨어를 정품화함으로써 사이버 위험을 줄일 수 있음은 확실하다. 또한, 이를 위한 국제적인 표준도 있다. 최근 갱신된 국제표준화 기구(ISO)의 SAM 표준은 소프트웨어를 포함한 전반적 IT 자산 관리(ITAM)를 위한 틀을 제공한다.[14]

최근의 한 사례에서 알 수 있듯이, ISO에서 조정한 SAM의 실행은 보안을 강화하는 강력한 도구이다. 미국에서, Equifax는 수 개월 전부터 알려져 있던 서버 한 대의 취약성에 대해 적절한 패치 작업을 하지 않아 사상 최대 규모의 데이터 침해가 발생하였고 이로 인해 4억 3,900만 달러로 추정되는 비용이 발생했으며, CEO와 CIO가 사퇴한 바 있다.[15] 전문가들의 보고에 따르면 이 업체에서 문제가 된 Apache 소프트웨어의 모든 활동을 추적하는 SAM 시스템이 있었다면 이러한 침해를 방지할 수 있었다.[16] 불법 소프트웨어의 사용을 방지함으로써 악성코드 노출을 최소화하는 것도 중요하지만 이 사례에서 알 수 있듯이 정품 소프트웨어를 쓰더라도 적절한 SAM 시스템을 갖추는 것은 필수적이다.

소프트웨어가 모두 정품이고 사업적 필요에 최적화됨으로써 SAM은 가동 휴지 시간의 감소와 손익의 개선이라는 추가적인 혜택을 가져다 준다. 또한 SAM을 이용하면 소프트웨어가 사업적 요건을 최적으로 충족하고 있음을 확인하고 클라우드 서비스 같은 신기술의 혜택을 누림으로서 업체들의 소프트웨어의 최대의 가치의 활용을 보장하는데 도움이 된다. 이들을 한데 모아 업체는 더욱 효율적이 될 것이며 비용을 절감할 수 있다. 연구 결과에 따르면 업체들은 견실한 SAM 프로그램을 실행함으로써 연간 소프트웨어 비용을 최대 30%까지 절감할 수 있다.[17]

조사에 따르면 SAM은 효과적인 투자이기도 한 것으로 밝혀졌다. 응답자들이 제공한 정보에 기초하여 IDC가 계산한 결과 소프트웨어 준법률을 단 20%만 높여도 (예컨대, 불법 소프트웨어 사용률을 24%에서 19%로 낮춤) 연간 매출액이 8,300만 달러인 업체의 (본 조사의 평균) 이익이 놀랍게도 11%가 늘어날 수 있다. 이렇게 막대한 손익의 개선은 준법률을 20% 증가시키기 위해 불법 소프트웨어를 정품화하는 비율보다 29배나 높은 것으로 추정된다.[18]

## 실질적 증거 사례들

**독일:**

직원이 12,000명 이상인 OSI International Foods는 효과적인 소프트웨어 라이선스 모델을 실행하여 정품화 이후의 비용을 30% 이상 줄였다.[19]

**러시아:**

Baltika Breweries는 러시아의 선두 맥주 업체로 독립된 양조장이 8곳 있으며 물리적 서비스와 클라우드 서비스를 모두 이용한다. SAM 프로그램을 시행하여 IT 시설을 최적화하고 사업용 응용 프로그램을 클라우드로 이전함으로써 연간 10만 달러를 절감하였다.[20]

**영국:**

런던의 Roehampt 대학교는 SAM 프로젝트에 착수해 더이상 이용하지 않는 소프트웨어와 과도하게 라이선스가 등록된 소프트웨어를 식별한 로드맵을 만들었다. 이를 통해 절감된 금액을 더욱 새롭고 역량이 우수하며 안전한 기술에 재투자하는 계획을 수립할 수 있었다. 프로젝트 전체 기간 중 절감 금액은 5백만 달러에 달할 것으로 추정된다.[21]

**미국:**

정부 기관도 혜택을 받을 수 있다. 예를 들어, NASA는 각 부서에 SAM의 우수 사례를 실행하게 하여 지난 6년 동안 1억 달러 이상을 절감했다.[22] NASA는 초기에 약간의 작업을 통해 전체 업무 영역에서의 디지털 전환으로 막대한 혜택을 누렸으며 납세자들의 세금을 절약할 수 있었다.

### 정부도 소프트웨어의 혜택을 확대하기 위해 실용적 조치를 취할 수 있다.

정부는 조직들이 취할 수 있으며 취해야 하는 조치에 더해 일련의 상식적이고 구체적인 조치를 취함으로써 불법 소프트웨어 사용률을 낮추고 경제 부문의 탄력을 크게 높일 수 있다. (15페이지에 자세히 설명하겠지만) 이러한 정부 주도의 적극적 노력에는 솔선수범, 정부 자체의 소프트웨어 자산 관리의 개선, 정부 계약업체들의 인증된 소프트웨어만의 사용의 보장 등이 있다.

BSA는 정부의 이러한 노력을 돕기 위해 정부 자체의 소프트웨어 자산 관리에 도움이 될 유용한 안내서를 개발했다.[23] 정부 자체가 합법적인 소프트웨어만 사용하며 마찬가지로 합법적 소프트웨어만 사용하는 계약업체들과만 거래를 하고 있음을 분명히 함으로써 공공 부문과 민간 부문 모두에 강하고 명료한 메시지를 보낼 수 있다.

## 불법 PC 소프트웨어 설치율과 상업적 가치

| | 불법 소프트웨어 설치율 | | | | 불법 소프트웨어의 상업적 가치(백만 달러) | | | |
|---|---|---|---|---|---|---|---|---|
| | 2017 | 2015 | 2013 | 2011 | 2017 | 2015 | 2013 | 2011 |
| **아시아 태평양** | | | | | | | | |
| 호주 | 18% | 20% | 21% | 23% | $540 | $579 | $743 | $763 |
| 방글라데시 | 84% | 86% | 87% | 90% | $226 | $236 | $197 | $147 |
| 브루나이 | 64% | 66% | 66% | 67% | $18 | $19 | $13 | $25 |
| 중국 | 66% | 70% | 74% | 77% | $6,842 | $8,657 | $8,767 | $8,902 |
| 홍콩 | 38% | 41% | 43% | 43% | $277 | $320 | $316 | $232 |
| 인도 | 56% | 58% | 60% | 63% | $2,474 | $2,684 | $2,911 | $2,930 |
| 인도네시아 | 83% | 84% | 84% | 86% | $1,095 | $1,145 | $1,463 | $1,467 |
| 일본 | 16% | 18% | 19% | 21% | $982 | $994 | $1,349 | $1,875 |
| 말레이시아 | 51% | 53% | 54% | 55% | $395 | $456 | $616 | $657 |
| 뉴질랜드 | 16% | 18% | 20% | 22% | $62 | $66 | $78 | $99 |
| 파키스탄 | 83% | 84% | 85% | 86% | $267 | $276 | $344 | $278 |
| 필리핀 | 64% | 67% | 69% | 70% | $388 | $431 | $444 | $338 |
| 싱가포르 | 27% | 30% | 32% | 33% | $235 | $290 | $344 | $255 |
| 한국 | 32% | 35% | 38% | 40% | $598 | $657 | $712 | $815 |
| 스리랑카 | 77% | 79% | 83% | 84% | $138 | $163 | $187 | $86 |
| 대만 | 34% | 36% | 38% | 37% | $254 | $264 | $305 | $293 |
| 태국 | 66% | 69% | 71% | 72% | $714 | $738 | $869 | $852 |
| 베트남 | 74% | 78% | 81% | 81% | $492 | $598 | $620 | $395 |
| 기타 아시아 태평양 지역 | 87% | 87% | 91% | 91% | $442 | $491 | $763 | $589 |
| **아시아 태평양 총계** | **57%** | **61%** | **62%** | **60%** | **$16,439** | **$19,064** | **$21,041** | **$20,998** |
| **중앙유럽 및 동유럽** | | | | | | | | |
| 알바니아 | 74% | 73% | 75% | 75% | $10 | $10 | $10 | $6 |
| 아르메니아 | 85% | 86% | 86% | 88% | $17 | $18 | $26 | $26 |
| 아제르바이잔 | 81% | 84% | 85% | 87% | $50 | $90 | $103 | $67 |
| 벨로루시 | 82% | 85% | 86% | 87% | $59 | $76 | $173 | $87 |
| 보스니아 | 61% | 63% | 65% | 66% | $24 | $24 | $21 | $15 |
| 불가리아 | 57% | 60% | 63% | 64% | $72 | $78 | $101 | $102 |
| 크로아티아 | 50% | 51% | 52% | 53% | $48 | $49 | $64 | $74 |
| 체코 공화국 | 32% | 33% | 34% | 35% | $149 | $150 | $182 | $214 |
| 에스토니아 | 41% | 42% | 47% | 48% | $16 | $16 | $20 | $25 |
| 마케도니아 | 63% | 64% | 65% | 66% | $15 | $15 | $19 | $22 |
| 조지아 | 81% | 84% | 90% | 91% | $22 | $25 | $40 | $52 |
| 헝가리 | 36% | 38% | 39% | 41% | $104 | $107 | $127 | $143 |
| 카자흐스탄 | 74% | 73% | 74% | 76% | $62 | $89 | $136 | $123 |
| 라트비아 | 48% | 49% | 53% | 54% | $22 | $23 | $29 | $32 |
| 리투아니아 | 50% | 51% | 53% | 54% | $35 | $37 | $47 | $44 |
| 몰도바 | 83% | 86% | 90% | 90% | $35 | $36 | $57 | $45 |
| 몬테네그로 | 74% | 76% | 78% | 79% | $6 | $6 | $7 | $7 |
| 폴란드 | 46% | 48% | 51% | 53% | $415 | $447 | $563 | $618 |
| 루마니아 | 59% | 60% | 62% | 63% | $151 | $161 | $208 | $207 |
| 러시아 | 62% | 64% | 62% | 63% | $1,291 | $1,341 | $2,658 | $3,227 |
| 세르비아 | 66% | 67% | 69% | 72% | $51 | $54 | $70 | $104 |
| 슬로바키아 | 35% | 36% | 37% | 40% | $51 | $55 | $67 | $68 |
| 슬로베니아 | 41% | 43% | 45% | 46% | $28 | $30 | $41 | $51 |
| 우크라이나 | 80% | 82% | 83% | 84% | $108 | $129 | $444 | $647 |
| 그 외 중앙유럽 및 동유럽 국가 | 86% | 87% | 89% | 90% | $69 | $70 | $105 | $127 |
| **중앙유럽 및 동유럽 총계** | **57%** | **58%** | **61%** | **62%** | **$2,910** | **$3,136** | **$5,318** | **$6,133** |
| **중남미** | | | | | | | | |
| 아르헨티나 | 67% | 69% | 69% | 69% | $308 | $554 | $950 | $657 |
| 볼리비아 | 79% | 79% | 79% | 79% | $94 | $98 | $95 | $59 |
| 브라질 | 46% | 47% | 50% | 53% | $1,665 | $1,770 | $2,851 | $2,848 |
| 칠레 | 55% | 57% | 59% | 61% | $283 | $296 | $378 | $382 |
| 콜롬비아 | 48% | 50% | 52% | 53% | $241 | $281 | $396 | $295 |
| 코스타리카 | 58% | 59% | 59% | 58% | $80 | $90 | $98 | $62 |
| 도미니카 공화국 | 75% | 76% | 75% | 76% | $74 | $84 | $73 | $93 |
| 에콰도르 | 68% | 68% | 68% | 68% | $132 | $137 | $130 | $92 |
| 엘살바도르 | 80% | 81% | 80% | 80% | $61 | $63 | $72 | $58 |
| 과테말라 | 78% | 79% | 79% | 79% | $165 | $169 | $167 | $116 |
| 온두라스 | 75% | 75% | 74% | 73% | $32 | $36 | $38 | $24 |
| 멕시코 | 49% | 52% | 54% | 57% | $760 | $980 | $1,211 | $1,249 |
| 니카라과 | 81% | 82% | 82% | 79% | $20 | $23 | $23 | $9 |
| 파나마 | 71% | 72% | 72% | 72% | $112 | $117 | $120 | $74 |
| 파라과이 | 83% | 84% | 84% | 83% | $76 | $89 | $115 | $73 |
| 페루 | 62% | 63% | 65% | 67% | $190 | $210 | $249 | $209 |
| 우루과이 | 67% | 68% | 68% | 68% | $51 | $57 | $74 | $85 |
| 베네수엘라 | 89% | 88% | 88% | 88% | $317 | $402 | $1,030 | $668 |
| 기타 라틴아메리카 국가 | 82% | 83% | 84% | 84% | $296 | $331 | $352 | $406 |
| **라틴아메리카 총계** | **52%** | **55%** | **59%** | **61%** | **$4,957** | **$5,787** | **$8,422** | **$7,459** |

| | 불법 소프트웨어 설치율 | | | | 불법 소프트웨어의 상업적 가치(백만 달러) | | | |
|---|---|---|---|---|---|---|---|---|
| | 2017 | 2015 | 2013 | 2011 | 2017 | 2015 | 2013 | 2011 |
| **중동 및 아프리카** | | | | | | | | |
| 알제리아 | 82% | 83% | 85% | 84% | $70 | $84 | $102 | $83 |
| 바레인 | 52% | 54% | 53% | 54% | $32 | $34 | $27 | $23 |
| 보스와나 | 80% | 79% | 79% | 80% | $22 | $23 | $20 | $16 |
| 캐머룬 | 80% | 82% | 82% | 83% | $20 | $21 | $9 | $9 |
| 이집트 | 59% | 61% | 62% | 61% | $64 | $157 | $198 | $172 |
| 이라크 | 85% | 85% | 86% | 86% | $107 | $120 | $116 | $172 |
| 이스라엘 | 27% | 29% | 30% | 31% | $165 | $161 | $177 | $192 |
| 코트디부아르 | 79% | 80% | 80% | 81% | $21 | $22 | $24 | $16 |
| 요르단 | 55% | 56% | 57% | 58% | $32 | $34 | $35 | $31 |
| 케냐 | 74% | 76% | 78% | 78% | $99 | $113 | $128 | $85 |
| 쿠웨이트 | 57% | 58% | 58% | 59% | $86 | $94 | $97 | $72 |
| 레바논 | 69% | 70% | 71% | 71% | $61 | $65 | $65 | $52 |
| 리비아 | 90% | 90% | 89% | 90% | $66 | $65 | $50 | $60 |
| 모리셔스 | 52% | 54% | 55% | 57% | $6 | $7 | $7 | $7 |
| 모로코 | 64% | 65% | 66% | 66% | $52 | $57 | $69 | $91 |
| 나이지리아 | 80% | 80% | 81% | 82% | $123 | $232 | $287 | $251 |
| 오만 | 60% | 60% | 60% | 61% | $56 | $59 | $65 | $36 |
| 카타르 | 47% | 48% | 49% | 50% | $64 | $72 | $77 | $62 |
| 레위니옹 | 38% | 39% | 39% | 40% | $2 | $2 | $1 | $1 |
| 사우디 아라비아 | 47% | 49% | 50% | 51% | $356 | $412 | $421 | $449 |
| 세네갈 | 74% | 75% | 77% | 78% | $12 | $12 | $9 | $9 |
| 남아프리카 | 32% | 33% | 34% | 35% | $241 | $274 | $385 | $564 |
| 튀니지 | 73% | 74% | 75% | 74% | $39 | $49 | $66 | $51 |
| 터키 | 56% | 58% | 60% | 62% | $208 | $291 | $504 | $526 |
| 아랍 에미리트 | 32% | 34% | 36% | 37% | $210 | $226 | $230 | $208 |
| 예멘 | 88% | 87% | 87% | 89% | $10 | $11 | $9 | $15 |
| 잠비아 | 80% | 81% | 81% | 82% | $4 | $4 | $3 | $3 |
| 짐바브웨이 | 89% | 90% | 91% | 92% | $7 | $7 | $4 | $4 |
| 기타 아프리카 국가 | 83% | 84% | 85% | 86% | $364 | $419 | $484 | $363 |
| 기타 중동 국가 | 85% | 84% | 85% | 87% | $478 | $569 | $640 | $536 |
| **중동 및 아프리카 총계** | **56%** | **57%** | **59%** | **58%** | **$3,077** | **$3,696** | **$4,309** | **$4,159** |
| **북미** | | | | | | | | |
| 캐나다 | 22% | 24% | 25% | 27% | $819 | $893 | $1,089 | $1,141 |
| 푸에르토리코 | 41% | 41% | 42% | 42% | $27 | $28 | $27 | $44 |
| 미국 | 15% | 17% | 18% | 19% | $8,612 | $9,095 | $9,737 | $9,773 |
| **북아메리카 총계** | **16%** | **17%** | **19%** | **19%** | **$9,458** | **$10,016** | **$10,853** | **$10,958** |
| **서유럽** | | | | | | | | |
| 오스트리아 | 19% | 21% | 22% | 23% | $121 | $131 | $173 | $226 |
| 벨기에 | 22% | 23% | 24% | 24% | $182 | $190 | $237 | $252 |
| 키프러스 | 44% | 45% | 47% | 48% | $14 | $14 | $19 | $19 |
| 덴마크 | 20% | 22% | 23% | 24% | $167 | $176 | $224 | $222 |
| 핀란드 | 22% | 24% | 24% | 25% | $166 | $171 | $208 | $210 |
| 프랑스 | 32% | 34% | 36% | 37% | $1,996 | $2,101 | $2,685 | $2,754 |
| 독일 | 20% | 22% | 24% | 26% | $1,566 | $1,720 | $2,158 | $2,265 |
| 그리스 | 61% | 63% | 62% | 61% | $173 | $189 | $220 | $343 |
| 아이슬란드 | 44% | 46% | 48% | 48% | $12 | $10 | $12 | $17 |
| 아일랜드 | 29% | 32% | 33% | 34% | $79 | $87 | $107 | $144 |
| 이탈리아 | 43% | 45% | 47% | 48% | $1,278 | $1,341 | $1,747 | $1,945 |
| 룩셈부르크 | 17% | 19% | 20% | 20% | $20 | $21 | $30 | $33 |
| 몰타 | 43% | 44% | 44% | 43% | $4 | $4 | $5 | $7 |
| 네덜란드 | 22% | 24% | 25% | 27% | $448 | $481 | $584 | $644 |
| 노르웨이 | 21% | 23% | 25% | 27% | $159 | $178 | $248 | $289 |
| 포르투갈 | 38% | 39% | 40% | 40% | $137 | $145 | $180 | $245 |
| 스페인 | 42% | 44% | 45% | 44% | $859 | $913 | $1,044 | $1,216 |
| 스웨덴 | 19% | 21% | 23% | 24% | $260 | $288 | $397 | $461 |
| 스위스 | 21% | 23% | 24% | 25% | $399 | $448 | $469 | $514 |
| 영국 | 21% | 22% | 24% | 26% | $1,421 | $1,935 | $2,019 | $1,943 |
| **서유럽 총계** | **26%** | **28%** | **29%** | **32%** | **$9,461** | **$10,543** | **$12,766** | **$13,749** |
| **전세계 총계** | **37%** | **39%** | **43%** | **42%** | **$46,302** | **$52,242** | **$62,709** | **$63,456** |
| 유럽연합 | 28% | 29% | 31% | 33% | $9,982 | $11,060 | $13,486 | $14,433 |
| BRIC (브라질, 러시아, 인도, 중국) * | 60% | 64% | 67% | 70% | $12,272 | $14,452 | $17,187 | $17,907 |

*BRIC 국가들은 브라질, 러시아, 인도, 그리고 중국이다.

# 세계적 추세

전 세계적으로, 수년에 걸친 교육과 집행이 이루어지고 소프트웨어 자산의 적절한 관리의 혜택에 대한 이해가 증진되면서 불법 소프트웨어의 사용이 다소 줄었다. 2015년에서 2017년까지 전세계 불법 소프트웨어의 사용률은 39%에서 2% 줄어 37%가 되었으며 불법 소프트웨어의 상업적 가치는 불변의 통화 기준으로 8% 줄어 463억 달러가 되었다.

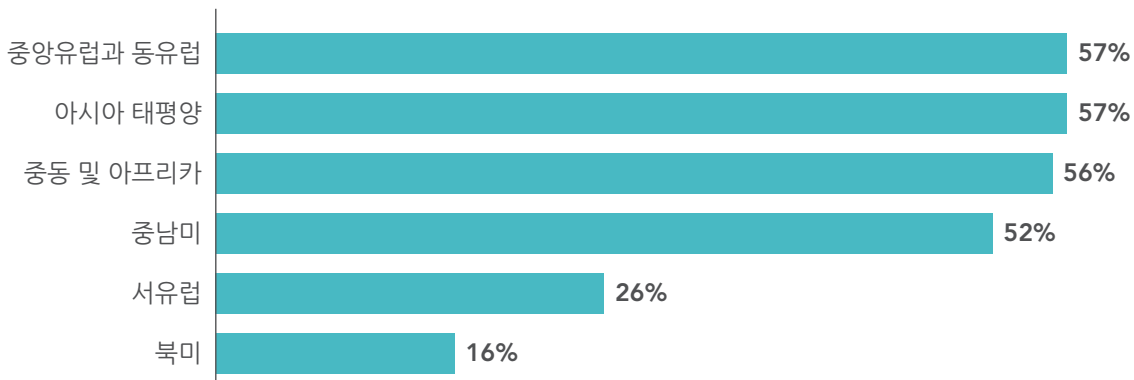
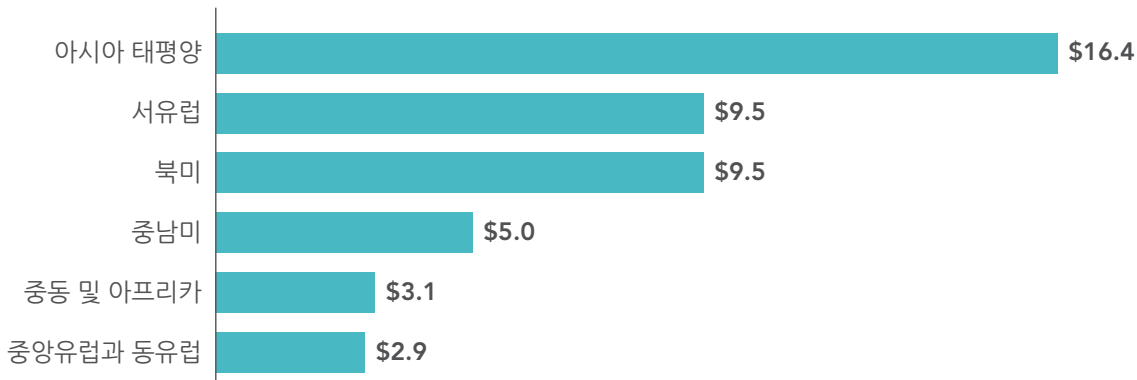
불법 소프트웨어 사용률 저하의 일부는 PC 납품의 감소에 기인하기도 하지만, IDC의 추정에 따르면 이 감소분의 60% 정도가 소프트웨어 규정 준수의 증가에서 비롯되었으며 이는 소프트웨어 규정 준수의 증가가 사업적으로도 사리에 맞을 수 있다는 것을 이해하는 사람이 많아졌다는 것을 시사한다. 이러한 진전에도 불구하고, 조사 대상의  절반 이상의 시장에서 대다수의 소프트웨어가 불법이어서 아직 많은 개선이 필요함을 알 수 있다.

모든 지역에서 불법 소프트웨어 사용률이 줄기는 했으나 신흥 시장을 제외하였다면 더욱 현저하게 줄어들었을 것이다. 신흥 시장은 불법 사용률이 평균인 61%보다 높으며 2017년 불법 소프트웨어 점유율은 2015년의 70%보다 높은 75%를 기록한다.

전 세계적으로 101개 시작에서 불법 사용률이 줄었으며 단 6개의 시장에서만 상승했다. 12개 국가에서 2017[24] 년에 불법 사용률이 3%가 줄었고, 중국과 베트남에서는 4%가 줄었는데 이는 이들 국가의 초기 불법 사용률이 높았음을 반영한다. 2017년 사용률을 2015년의 사용률로 나눈 비율 기준으로 보면 가장 크게 감소한 곳은 선진국으로 미국, 호주, 오스트리아, 일본, 룩셈부르크, 뉴질랜드, 싱가포르, 스웨덴에서 10% 이상 감소하여 경제적 효과 및 사이버 보안 효과를 달성하는데 도움을 주었다.

### 불법 소프트웨어 사용률이 감소될 때 모든 지역이 혜택을 받는다.

- **아시아-태평양:** 아시아-태평양 지역은 소프트웨어의 57%가 불법으로 2015년 대비 불법 사용률이 4% 감소했음에도 불구하고 전체 비율은 최고 수준이다. 따라서, 이 지역의 불법 소프트웨어의 상업적 가치는 충격적인 164억 달러에 달하며 세계 어느 지역보다도 높고 전 세계 불법 소프트웨어의 상업적 가치의 3분의 1을 차지하고 있다. 이 지역 내에서도 68억 달러의 불법 소프트웨어 상업적 가치가 중국 한 곳에서만 기록되었다.
- **중동부 유럽:** 중동부 유럽 지역은 아시아-태평양 지역과 함께 불법 소프트웨어 사용률이 57%로 가장 높은 수준이며 2015년 대비 불과 1% 하락했다. 지역 내에서도 불법 소프트웨어가 사용되는 정도에는 차이가 많았다. 아르메니아가 85%의 불법 소프트웨어 사용률을 보여 가장 높았으며 83%의 몰도바와 82%의 벨로루시가 뒤를 이었다. 대조적으로, 체코 공화국은 32%로 이 지역에서 가장 낮았으며 슬로바키아가 35%로 뒤를 이었다. 하지만 러시아는 13억 달러의 상업적 가치를 지니고 계속 이 지역 내 최고의 불법 소프트웨어 사용률을 계속 보이고 있다.
- **중동 및 아프리카:** 중동 및 아프리카는 전반적으로 1% 줄어 56%가 되었으나 2개 시장에서의 불법 사용률은 1% 상승했고 4개의 시장에서는 변화가 없었다. 이 지역은 여전히 세계 최고의 지역보다 1% 낮은 수준이다. 이 지역 내에서는 각 90%와 89%를 보이는 리비아와 짐바브웨를 포함한 몇 개국이 세계에서 불법 소프트웨어 사용률이 가장 높은 국가에 속한다. 이에 비해 아랍 에미리트 연합(32%)과 남아프리카(32%), 이스라엘(27%)은 정품 소프트웨어의 혜택을 크게 누리고 있다.

불법 소프트웨어 평균 사용률

불법 소프트웨어 사용의 상업적 가치(10억 단위)

- **라틴아메리카:** 이 지역에서는 52%의 소프트웨어가 불법이며 이는 2015년 대비 3% 줄었다. 이러한 불법 소프트웨어의 상업적 가치는 약 50억 달러에 달한다. 가장 비율이 높은 국가는 89%의 베네수엘라(세계에서 두 번째로 높음), 81%의 니카라과 그리고 80%의 엘살바도르가 포함된다. 이에 비해 46%의 브라질, 48%의 콜롬비아, 49%의 멕시코는 현재 낮은 불법 사용률의 혜택을 누리고 있다. 실제로, 멕시코는 2015년 대비 불법 사용률이 3% 하락했다. 이 지역에서 브라질의 사용률이 가장 낮기는 하지만 이 지역에서 가장 큰 국가여서 불법 소프트웨어의 상업적 가치가 17억 달러에 달해 이는 이 지역 최고의 상업적 가치이다.
- **서유럽:** 서유럽의전체적인 불법 사용률은 2% 하락해 26%가 됐다. 아일랜드는 가장 큰 감소율인 3%를 기록하면서 29%의 불법 사용률을 기록하게 되었다. 그리스는 61%의 엄청난 불법 사용률을 기록하면서 이 지역에서 계속해서 특이한 기록을 유지하고 있다. 이 지역에 위치한 여러 나라들은 상업용 소프트웨어의 가치를 최대화 할 수 있었고 세계에서 가장 낮은 불법 사용률을 유지함으로써 사이버 보안위험을 낮출 수 있었다. 이들 가운데 룩셈부르크는 17%, 스웨덴은 19%, 오스트리아는 19%, 덴마크와 독일은 20%, 그리고 스위스는 21%를 기록하고 있다. 조사된 20개 국가 중 16개의 국가에서는 2015년 대비 2% 이상이 감소했다. .
- **북미:** 북미는 크기로 인해 95억 달러라는 거대한 상업적 가치를 기록하고 있지만 계속해서 16%로 가장 낮은 비율을 유지하고 있다.

# 소프트웨어 자산 관리: 귀하의 조직을 위험으로부터 보호하고 가치를 증대시키는 방법

사업체들은 기술 자산으로부터 파생할 수 있는 혜택을 계속해서 최대화하고 불법 소프트웨어와 연관된 악성코드를 줄이기 위한 바로 적용할 수 있는 세계적 우수 사례들을 보유하고 있다. 연구에 의하면, 강력한 소프트웨어 자산 관리(SAM) 프로그램을 실행하면서 조직들은 소프트웨어 비용을 한 해 30%까지 줄일 수 있다.[25]

2017년 판 ISO/IEC 19770-1 표준은 SAM을 위한 효과적인 ISO 제휴 시스템의 실행을 위해 총체적인 접근법을 제공한다. 표준을 실행함으로써 점진적 세 단계의 이행에 있어 지속적으로 과정을 개선할 수 있다. 이런 단계식 접근법은 조직들로 하여금 적절하게 단계적 이행을 가능하게 한다. 이 표준화는 (1) 선택된 단계에 맞춰진 전반적 이행 계획을 창출하면서; (2) 관리되고 규율적인 방식으로 계획을 실행하고; (3) 계획 대비 진행 경과를 평가하고 (4) 지속적인 개선을 보장하기 위해 필요한 계획을 조절하는 산업표준 과정을 통한 단계적 적용을 고려한다.

1 단계

### 신뢰할 수 있는 데이터

첫 단계는 무엇을 보유하고 있는지에 대하여 철저히 이해하여 종합적으로 관리할 수 있도록 하는 것이다. 이는 소프트웨어 면허 동의서의 준수를 위해 시스템에 있는 소프트웨어를 평가하는 것에서 시작한다.  면허 관리와 더불어 이 단계는 또한 조직들로 하여금 변화 관리, 데이터 관리, 보안 관리에 필요한 프로세스들을 개발하는 데 도움을 준다.

2 단계

### 라이프 사이클 통합

두 번째 단계는 첫 번째 단계에서 진행이 되며 조직들로 하여금 전체 IT 자산의 라이프 사이클에 걸친 관리를 세부 사양에서부터 인수, 개발, 출시, 배치, 운영 그리고 폐기까지의 관리를 개선하여 효율성 및 비용 대비 효과를 높이도록 도움을 준다.

3 단계

### 최적화

세 번째 단계는 계약과 재정적 관리 같은 기능 분야에 집중하여 효율성 및 비용 대비 효과를 높이도록 도움을 준다.

## 정부가 취할 수 있는 단계들

최신 기술 주도적 진보의 장점을 최대한 활용할 수 있는 조직들이 제공할 수 있는 방대한 새로운 직업들, 세금을 기반으로 한 개선들 그리고 경제적 혜택들을 활용하기 위해 정부는 그들이 불법 소프트웨어 사용률을 줄이고 경제 분야에 더욱 뛰어난 탄력성을 가져다 줄 수 있도록 취할 수 있는 일련의 상식적 그리고 구체적 조치를 보유하고 있다.

### 1 예를 들어:

정부는 세계 최대의 소프트웨어 사용자이다. 모든 조직들과 함께 그들은 위험을 감소하고, 기술 책임성을 개선하고 SAM을 채택함으로써 혜택을 받을 수 있다. 정부는 또한 주정부 소유의 기업들과 계약업체 그리고 공급업체에게 SAM과 완전히 합법적인 소프트웨어의 사용을 홍보할 수 있다.

### 2 공교육과 인지력의 개선

정부, 회계사, 회계감사자, 업계 컨설턴트, 무역 협회 그리고 사업 조직들은 조직을 대상으로 소프트웨어 면허 규정의 준수와 불법 소프트웨어 설치와 사용의 위험성에 대하여 교육을 시켜야 한다.

### 3 새로운 혁신을 다룰 수 있는 법률의 현대화:

클라우드의 출현과 네트워크로 연결된 휴대 장치들의 확산으로 소프트웨어는 혁신적인 새로운 방식으로 저장되고 전달되며 사용되고 있다. 정책 수립자들은 전달의 형식 혹은 수단에 상관없이 정보가 보호되도록 보장해야 한다.

### 4 시행에 도움이 되는 환경의 조성:

정부는 소프트웨어 저작권 침해를 줄이기 위해 법적 체계가 투자자들 사이에 협력을 조정하고 증진시키기 위한 효과적인 수단을 제공하도록 보장해야 한다.

## 클라우드로 전환하면서 기회를 가속화하기

클라우드는 컴퓨터 관련 자원들을 구입하고 판매하고 전달하는 방식을 근본적으로 변혁시켜 놓았기에 한 시대의 가장 변혁적인 기술 중 하나로 부상하고 있다. 이는 한때 대규모의 조직들만이 이용할 수 있었던 기술들을 이제는 작은 사업체나 성장하는 업체 등 거의 모든 업체들이 이용할 수 있도록 해준다. 이 클라우드를 통해 가능한 디지털 능력은 오늘날 기업들이 사용하고 있는 클라우드 기반 서비스의 양과 질 그리고 다양성에 있어서 폭발적인 성장을 견인했다. 평균 기업들이 사용하는 클라우드 기반 응용 프로그램의 수는 3년간 3배로 성장한 것으로 추정되고 있다.[26] 많은 경우에 클라우드는 인터넷을 통해 이용 가능한 서비스로서 전통적이고 향상된 소프트웨어 기능성을 제공해 주고 있다. 실제로 IDC의 추정에 의하면 클라우드는 세계적으로 현재 22%의 소프트웨어 기능성을 제공하고 있다.

비용 절감, 개선된 신속성, 단순성, 강화된 보안성을 갖고 있는 클라우드의 원천적 역량으로 인해 사업체들은 클라우드 서비스로 몰려들고 있다.

- **클라우드는 비용 대비 효과적이다:**성공적으로 클라우드로 전환한 정보기술 업체들은 계속해서 방대한 데이터 센터를 운영하고 대부분의 응용 프로그램을 현장에서 호스팅하는 동일 업계의 업체들보다 평균적으로 21%가 낮은 정보기술 비용을 소비하고 있다.[27] 이들 업체의 지도자들은 클라우드를 통해 기존의 하드웨어 설비를 업그레이드하고 유지하기 위해 값비싼 자본 투자를불필요하게 해주어 클라우드가 정보기술 비용을 줄여줄 수 있다는 것을 인지하고 있다. 조직들은 또한 클라우드가 필요한 자원에 대해서만 지불할 수 있게 해주고 동시에 거의 무한정으로 인터넷에서 전산 능력을 활용하고 저장을 할 수 있게 해주기에 비용을 절감하고 있다.
- **클라우드는 안전하고 융통성이 있다:** 클라우드의 독특한 설계는 전산 관련 자료들을 구매, 판매, 전달하는 방식을 바꿀 뿐만 아니라 응용 프로그램을 세계적으로 언제 어디에서나 모든 장치를 통해서 이용할 수 있게 만드는 전대미문의 융통성을 제공한다. 어떤 이들에게 클라우드의 가장 위대한 장점은 전통적 모델에 클라우드가 제공하는 주요 보안의 개선이다. 클라우드 제공업체들은 개인 고객들보다 더 광범위한 위협의 상황을 파악하여 조기에 위험을 식별할 수 있고 더 정교한 보안 기술을 전개할 수 있다. 그들은 또한 진보된 위협 보호 기술을 전개하고 사용하지 않거나 이동 중인 데이터를 암호화하고 새로 발견된 위협으로부터 더욱 신속히 시스템을 보호할 수 있는 업데이트를 자동화하여 보안 기능을 최대화할 수 있다. 이러한 기능들은 데이터의 회복력을 개선시키고 조직의 보안력을 강화시킬 수 있다.
- **SAM은 클라우드로 이전할 수 있는 기회를 제공한다:** 클라우드가 기업 전반에 걸쳐 새로운 디지털 기회를 견인하게 하는 전대미문의 잠재성을 사업체들에 제공하면서 SAM은 클라우드로 전환을 가속화 시켜주는 중요한 요인이 되었다. SAM은 다양한 핵심적 방법으로 조직들이 클라우드 서비스의 이용을 준비할 수 있도록 도움을 준다. SAM은 조직들이 면허 전략을 최적화하고 클라우드로 이전하면서 가능한 추가적 비용절감에 대한 통찰력을 획득하고 클라우드 서비스를 이용하는 데 필요한 전략을 개발하도록 도움을 준다. 이러한 전략을 갖추어야만 업체들은 클라우드 서비스로부터 최대한의 잠재력을 확보할 수 있다. 예를 들어, 런던 남서쪽에 위치한 Roehampton 대학은 종합적인 클라우드 이전 전략을 개발함으로써 SAM을 활용했다. 대부분의 대학 정보기술 기반을 클라우드로 원활하게 옮김으로써 Roehampton 대학은 데이터 센터 장비로의 새로운 투자를 하지 않아도 되었고 새로운 융통성과 확장성을 확보할 수 있었으며 보안을 개선할 수 있었고 10년 동안 40%의 비용(대략 470만 달러)을 절감할 수 있었다.[28]

많은 사업체들이 시장에서 전략적 우위를 줄 수 있는 클라우드로 전환해감에 따라, 그들은 원활한 전환에 필요한 근본적인 단계들을 종종 찾고 있다. SAM을 이행하는 것은 기업들이 클라우드로 옮김으로써 얻을 수 있는 변형적 이익을 가속할 수 있도록 도움을 준다.

# 방법론

BSA 글로벌 소프트웨어 조사는 특정 년도에 (이 경우에는 2017년) 110개국과 지역 경제에 걸쳐 개인용 컴퓨터에 설치된 불법 소프트웨어의 양과 가치를 계량화한다. BSA는 또한 소프트웨어 면허 관련 관점에 대한 통찰력을 제시하고 불법 소프트웨어 사용을 줄일 시의 직접적인 경제적 영향에 대한 새로운 통찰력을 제시하기 위해 이 조사는 또한 32개국에 걸쳐 집에서 혹은 직장에서 컴퓨터를 사용하는 소비자와 직장인들로부터 수집한 22,500개 이상의 답변을 포함하는 국제적 조사를 포함하고 있다. 보고서를 편집하기 위해 BSA는 전 세계에 걸쳐 정품 및 불법 소프트웨어를 측정하고, 이해하고, 평가하기 위해 세계적인 선두 독립 연구 업체 중 하나인 IDC와 긴밀히 제휴하였다.

불법 소프트웨어 사용의 규모와 범위를 명료하게 측정하는 것이 BSA의 난제였다. 이 연구가 세계 저작권 침해에 관한 가장 정교한 평가중의 하나로 인정받고 있지만 BSA와 파트너들은 계속해서 데이터 신뢰성을 개선시킬 수 있는 새로운 방법들을 모색하고 있다. 2011년에 두 명의 저명한 정보기술 경제 연구원들과 협조하여 BSA는 입력 정보를 개선하고 불법 소프트웨어의 사용을 가장 정확하게 추정할 수 있도록 여러 가지 방식으로 조정을 하였다.

## 소프트웨어 사용자에 대한 세계적 조사

BSA 세계 소프트웨어 조사의 주된 요소는 2017년 11월에 IDC가 시행한 세계적 조사로서 22,500 이상의 가구와 업체의 컴퓨터 사용자들을 대상으로 시행하였다. 이 조사는 32개의 시장에 걸쳐 온라인이나 전화로 시행되었는데 이 32개국 시장은 전 세계의 지역, 정보기술의 수준 그리고 지역과 문화적 다양성을 대표한다. 더불어 23개국 2,300명의 정보기술 관리자들을 대상으로 병행 조사가 이루어졌다.

이들 조사는 부분적으로 각 나라의 “소프트웨어의 양 (software load)”을 측정하기 위해서 사용되었다. 즉, 상업용 공개 소스 그리고 혼합된 소스 프로그램을 포함해서 각 컴퓨터에 설치된 소프트웨어 프로그램의 대략적 수를 파악하기 위해 사용되었다. 얼마나 많은 소프트웨어 패키지와 어떤 종류가 작년에 그들 컴퓨터에 설치되었는지, 몇 퍼센트가 새로운 패키지 혹은 업데이트였는지, 컴퓨터를 구입할 때 포함되었는지 아니면 새로운 컴퓨터에 설치되었는지 또는 2017년 이전에 입수했는지에 대한 질문이 응답자들에게 주어졌다. 개인 소비자와 사업체 사용자들에게 이들 질문을 제시하였다.

또한 이들 조사는 지적 재산, 불법 소프트웨어의 사용 그리고 기타 대두되고 있는 기술적 문제와 관련된 사회적 관념과 행동을 평가하기 위해 시행된다. 이러한 통찰력은 전 세계적으로 불법 소프트웨어의 사용의 근간을 이루는 역동성에 관한 새로운 시각을 매년 제시한다.

조사대상 국가들은 매년 전 세계적 범위를 최대한 포괄하기 위해서 순환 전략을 사용하여 선택된다. 11개의 우선 순위의 시장이 각 연구 주기에 맞추어 조사되고 있고 52개국의 나라들은 최소 매번 두 번 혹은 세 번의 주기에 한 번은 조사가 된다. 나머지 국가들은 상황에 맞게 선택된다. 연구 주기에 있어 전체 조사 인구 대상은 전체 소프트웨어의 85% 이상을 그리고 90% 정도의 구입 소프트웨어를 차지하고 있고 대부분의 시장이 적어도 3년의 연구 주기에 있어 한번은 조사되도록 하고 있다.

## 불법 소프트웨어 설치율 계산

2003년부터 BSA는 불법 소프트웨어 사용률과 불법 설치의 상업적 가치를 판단하기 위해 정보기술 업계의 시장 통계와 예측치를 제공하는 선두 업체인 IDC와 제휴해오고 있다.

한 국가에서 발생하고 있는 사용률과 상업적 가치를 파악하기 위한 기본적 방법은 다음과 같다:

1. 한 해에 걸쳐 얼마나 많은 컴퓨터 소프트웨어가 소비자와 기업에 배치되었는지를 확인한다.
2. 당해에 얼마나 구입을 하였는지 혹은 합법적으로 획득되었는지 (공개 소스, 무료 혹은 보충 면허를 통해서) 그리고 이를 기업과 소비자의 사용 별로 다시 분류한다.
3. 불법 소프트웨어의 양을 확인하기 위해 하나에서 다른 하나를 뺀다. 이 양이 확인되면 불법 사용률이 설치된 전체 소트프웨어에서 몇 퍼센트나 차지하는지 계산이 된다.

**불법률**
**=**
**불법 소프트웨어 수량 /**
**설치된 전체 소프트웨어 수량**

**설치된 전체 소프트웨어 수량**
**=**
**소프트웨어를 갖춘 컴퓨터 수량 X**
**각 컴퓨터 당 소프트웨어의 수량**

설치된 소프트웨어의 전체 수량 즉, 분모를 계산하기 위하여 IDC는 한 국가에 얼마나 많은 컴퓨터가 있는지 그리고 한 해에 그 컴퓨터 중 얼마나 많은 컴퓨터들이 소프트웨어를 받았는지 판단한다. IDC는 92개 나라를 포괄하는 "컴퓨터 추적기(PC Trackers)"라는 분기별 연구 제품을 통해 이 정보를 추적한다. 남은 몇몇 국가들은 이 연구를 위해 매년 조사된다.

일단 IDC가 얼마나 많은 컴퓨터가 있는지 (개인 컴퓨터와 사업용 컴퓨터 모두) 수량을 확인하고 조사를 통해 수집된 소프트웨어 설치 데이터를 활용하여 각 국가에 설치된 전체 합법 및 불법 소프트웨어의 수량을 확인할 수 있다.

조사하지 않은 국가에 있는 소프트웨어 양을 측정하기 위해 IDC는 다양한 소프트웨어의 설치율을 보유하고 있는 나라들의 유사한 특징을 찾기 위한 클러스터 분석 기술을 사용하여 조사가 되지 않은 국가에서의 소프트웨어 사용량을 정한다. IDC는 조사된 국가들에서 확인된 소프트웨어의 설치량과 ICT 발전 지표라 불리는 국제 통신 조합에서 발행한 신흥 시장 측정 점수와의 상관 관계를 확인하고 이를 조사되지 않은 국가들과 비교하기 위하여 집단별로 나누어 검증한다.

불법 소프트웨어의 수량을 알기 위해서, 즉, 위에 언급한 방정식의 분자를 알기 위해서 IDC는 합법적으로 획득한 소프트웨어 시장의 가치를 파악해야 한다. IDC는 정기적으로 대략 80개 국가로부터 추출한 소프트웨어 시장 데이터를 출판하고 세관 기록을 근거로 하여 대략 20개 국가를 추가로 조사한다. 나머지 국가들에 대해서는 IDC는 이 연구의 목적상 연간 연구를 시행한다. 이 연구는 합법적으로 획득한 소프트웨어 시장의 가치를 제공한다. 이 가치는 개인 소비자와 사업체 사용자로 나뉘어진다.

소프트웨어 시장 가치를 단위 수로 전환하기 위해 IDC는 국가의 모든 개인 소비자와 사업체 컴퓨터에 설치된 각 소프트웨어의 평균 가격을 산출한다. 이는 보안, 사무실 자동화, 운영체계 등을 포함하여 소매가, 볼륨 라이선스, OEM, 무료 그리고 공개 소스와 같은 제품의 매트릭스 전반에 걸친 국가별 소프트웨어 가격 매트릭스를 개발하여 처리한다.

IDC 가격 정보는 가격 추적기 및 지역 분석가의 연구를 통해서 확보한다. OEM과 소매, 소비자와 기업 간의 가중치는 IDC 조사에서 확보한다. IDC는 두 개의 매트릭스를 곱하여 최종 혼합 평균 소프트웨어 단가를 산출한다.

합법적 소프트웨어의 전체 수량의 확인을 위해 IDC는 다음의 공식을 적용한다:

**합법적 소프트웨어 수량**
**=**
**소프트웨어 시장 가치 /**
**소프트웨어의 평균 단가**

2011년 IDC는 평균 소프트웨어 단가의 산출을 검증하기 위해 다양한 방법을 시행했다. 25개국에 있는 분석팀들은 IDC의 계산 가치를 교차 확인하기 위해 범주 및 사용자에 따라서 (소비자 또는 사업체) 그리고 획득 유형에 따라 (예를 들어, 소매, 볼륨 라이선스, 무료/공개 소스) 소프트웨어 가격에 대한 추가적인 정보를 제공했다. 매년 정보가 수집되는 나라들을 교체하면서 IDC는 주기적으로 소프트웨어 가격을 재조정하고 업계의 수익에서 합법적

소프트웨어의 더욱 정확한 추정 가격을 제공할 수 있다.

마지막으로 총 소프트웨어 수량에서 합법적 소프트웨어의 수량을 빼면 한 해 동안 설치된 불법 소프트웨어의 수량이 계산된다.

불법소프트웨어 수량
=
전체 설치된 소프트웨어 수량
-
합법적 소프트웨어 수량

이러한 과정은 기본 비율 방정식의 근간을 이루는 데이터를 제공한다.

## 불법 소프트웨어의 상업적 가치의 계산

불법 소프트웨어의 상업적 가치는 불법 소프트웨어 사용 규모에 대한 또 다른 측정치를 제공하고 소프트웨어의 영역에서 발생하는 변화에 대하여 중요한 연도별 비교를 가능하게 한다.

상업적 가치는 IDC가 소매가, 볼륨 라이선스, OEM, 무료, 공개 소스, 소비자 또는 사업체 등을 포함한 소프트웨어의 평균 가격을 산출하는 데 사용하는 동일한 가격들을 혼합하여 계산한다. 평균 소프트웨어의 단가는 일반 상점의 소매 가격보다 낮다.

설치된 소프트웨어의 전체 수량과 합법적으로 설치된 소프트웨어의 수량과 불법으로 설치된 소프트웨어의 수량 그리고 각 소프트웨어의 평균 가격을 산출하여 IDC는 불법 소프트웨어의 상업적 가치를 계산해낼 수 있다.

## 포함되는 소프트웨어

BSA 글로벌 소프트웨어 조사는 데스크탑, 랩탑 그리고 넷북과 같은 극소형 휴대 컴퓨터를 포함하여 컴퓨터에서 실행되고 있는 소프트웨어 불법 설치율을 계산한다.

이는 운영체계, 데이타베이스와 보안 패키지, 사업 응용 프로그램 같은 시스템 소프트웨어와 또한 게임, 개인 재무관리 그리고 참고 소프트웨어와 같은 소비자 응용 프로그램도 포함하고 있다. 이 연구는 또한 상용으로 공유되는 합법적 무료 소프트웨어와 오픈 소스의 가용성도 고려하고 있다. 이는 일반적으로 무료이며 또한 상업적 제품에 이용될 수 있다.

그러나 태블릿이나 스마트폰에 내장된 소프트웨어를 포함하지는 않는다. 또한 서버나 본체에서 실행되는 소프트웨어, 정해진 장치의 드라이버 그리고 스크린 세이버 등의 유료 소프트웨어나 일반적으로 사용자가 소프트웨어 프로그램으로 인식하는 다운로드가 가능한 무료 유틸리티는 제외된다.

이 연구는 개인 컴퓨터에 설치되었을 소프트웨어를 대신할 수 있는 서비스로서의 소프트웨어(SaaS) 그리고 서비스로서의 플랫폼(PaaS) 같은 클라우드 전산 서비스를 포함한다. 이 연구는 학교에 공급하기 위한 정부의 다량 구매와 같은 공식으로 적법화된 프로그램의 일부로 판매되는 소프트웨어를 포함한다.

## 환율의 영향

2009년 전의 가치 도표에서의 달러 수치는 바로 전년도 달러의 경상 달러로 기록되었다. 예를 들어, 불법 소프트웨어의 2007년 가치에는 비교를 쉽게 하기 위해 2006년 달러를 게재하였다. 2009년 BSA는 조사되는 해의 달러의 가치를 게재하기로 정하였다. 따라서 2009년 가치는 2009년 달러의 가치이며 2017년의 가치는 2017년의 달러 가치이다. 이전의 가치를 현재 달러의 가치로 다시 수정하여 게재하지는 않는다.

이는 시간이 지남에 따라 변하는 가치를 평가할 시 중요하다. 일부 가치의 변동은 실제 시장의 역동성에 기반하고 일부는 해마다 변하는 환율에 기반하고 있다.

## 엔드 노트

1 "Gartner Says Organizations Can Cut Software Costs by 30 Percent Using Three Best Practices," Gartner (July 19, 2016), available at www.gartner.com/newsroom/id/3382317 and "Demonstrating the Business Value of Software Asset Management and Software License Optimization," Gartner, available at http://imagesrv.gartner.com/media-products/pdf/flexera/flexera_issue1.pdf.

2 McAfee Labs Threat Report (March 2018), available at https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2018.pdf

3 "Cyber-Attacks Occurring More Frequently and With Greater Sophistication, NTT Security Report Finds," Security InfoWatch (August 9, 2017), available at www.securityinfowatch.com/press_release/12358487/cyber-attacks-occurring-more-frequently-and-with-greater-sophistication-ntt-security-report-finds.

4 *Internet Security Threat Report*, Symantec (April 2017), available at www.symantec.com/security-center/threat-report.

5 In 2015, 43 percent of cyber-attacks worldwide were against small businesses with less than 250 workers. Elizabeth MacDonald, "Cyber Attacks on Small Businesses on the Rise," *Fox Business* (April 26, 2016), available at www.foxbusiness.com/features/cyber-attacks-on-small-businesses-on-the-rise.

6 *Internet Security Threat Report*, Symantec (April 2017), available at www.symantec.com/security-center/threat-report.

7 Ponemon Institute, *2017 Cost of Cyber Crime Study*, available at www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf.

8 "Global Cybercrime Costs Top $600 Billion," DarkReading (February 21, 2018), available at https://www.darkreading.com/attacks-breaches/global-cybercrime-costs-top-$600-billion-/d/d-id/1331106.

9 M-Trends 2013: Attack the Security Gap, Mandiant (2013), available at https://www.fireeye.com/current-threats/annual-threat-report/mtrends/rpt-2013-mtrends.html

10 Ponemon Institute, *2017 Cost of Cyber Crime Study*, available at www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf.

11 Paul Mozur, "China, Addicted to Bootleg Software, Reels From Ransomware Attack," *New York Times* (May 15, 2017), available at www.nytimes.com/2017/05/15/business/china-ransomware-wannacry-hacking.html.

12 "China's Fondness for Pirated Software Raises Risks in Attack," *Phys Org* (May 16, 2017), available at https://phys.org/news/2017-05-china-fondness-pirated-software.html.

13 "Jakub Kroustek, a malware researcher with Avast, a security software company in the Czech Republic, said in a blog post that Russia was the most-affected country so far [from a malware attack]."Elizabeth Dwoskin and Karla Adam, "More Than 150 Countries Affected by Massive Cyberattack, Europol Says," *Washington Post* (May 14, 2017), available at https://www.washingtonpost.com/business/economy/more-than-150-countries-affected-by-massive-cyberattack-europol-says/2017/05/14/5091465e-3899-11e7-9e48-c4f199710b69_story.html.

14 International Organization for Standardization, *ISO/IEC 19770-1:2017 Information Technology—IT Asset Management*, available at www.iso.org/standard/68531.html.

15 "Equifax Breach to Cost Total of $439M," PYMNTS (March 5, 2018), available at www.pymnts.com/news/security-and-risk/2018/equifax-cost-275m/.

16 "How Could ITAM Have Helped the Equifax CIO?" *The ITAM Review* (October 19, 2017), available at www.itassetmanagement.net/2017/10/19/equifax-itam/.

17 "Gartner Says Organizations Can Cut Software Costs by 30 Percent Using Three Best Practices," Gartner (July 19, 2016), available at www.gartner.com/newsroom/id/3382317 and "Demonstrating the Business Value of Software Asset Management and Software License Optimization," Gartner, available at http://imagesrv.gartner.com/media-products/pdf/flexera/flexera_issue1.pdf.

18 These important benefits are derived from the combination of better security by reducing malware that may accompany unlicensed software, fewer disruptive audits that take precious time to respond to, reduced legal risks around license compliance violations, better IT productivity by eliminating outdated or unsupported software, more trusted brand identity by avoiding risky behavior, and better relationships with vendors.

19 With a more effective licensing model in place, OSI reduced costs by more than 30 percent and achieved 100 percent compliance with Microsoft guidelines. See "OSI International Foods Increases Software License Visibility and Reduces Costs by 30 Percent," Microsoft Customer Solution Case Study, available at http://download.microsoft.com/download/7/F/1/7F18B556-BC4D-4B5C-BAB8-9386515BF1EB/Germany-OSI_International_Foods.doc.

20 Baltika conducted a SAM project that now saves them $100,000 per year in the workstation, software, and servers. See "Baltika Breweries Unlocks the Power of Microsoft Technologies Through SAM," YouTube, available at www.youtube.com/watch?v=yocvI9nl8o0&feature=youtu.be; and "Software Asset Management Customer Evidence," Microsoft, available at www.microsoft.com/en-us/sam/customers.aspx.

21 "University of Roehampton Benefits From Azure Migration Through Microsoft SAM," YouTube, available at https://www.youtube.com/watch?v=hAHHvZ_8zz4&feature=youtu.be; and "Software Asset Management Customer Evidence," Microsoft, available at https://www.microsoft.com/en-us/sam/customers.aspx.

22 Using a specialized SAM tool and other strategies, the space agency uncovered software consolidation opportunities. For NASA, it meant eliminating duplicate software licenses and negotiating better prices for the software it already buys. "How NASA Saved $100 Million on Software Licenses," *FedTech* (February 23, 2017), available at https://fedtechmagazine.com/article/2017/02/how-nasa-saved-100-million-software-licenses.

23 See BSA | The Software Alliance, *Government Guide for Software Asset Management*, available at www.bsa.org/~/media/Files/Tools_And_Resources/Guides/SoftwareManagementGuide/SoftwareManagementGuide_Government.pdf.

24 Azerbaijan, Belarus, Bulgaria, Georgia, Hong Kong, Ireland, Mexico, Moldova, Philippines, Singapore, South Korea, and Thailand.

25 "Gartner Says Organizations Can Cut Software Costs by 30 Percent Using Three Best Practices," Gartner (July 19, 2016), available at www.gartner.com/newsroom/id/3382317 and "Demonstrating the Business Value of Software Asset Management and Software License Optimization," Gartner, available at http://imagesrv.gartner.com/media-products/pdf/flexera/flexera_issue1.pdf.

26 Ajmal Kohgadai, "12 Must-Know Statistics on Cloud Usage in the Enterprise," SkyHigh Networks, available at https://www.skyhighnetworks.com/cloud-security-blog/12-must-know-statistics-on-cloud-usage-in-the-enterprise/.

27 "Cloud Users Enjoy Significant Savings," Computer Economics (April 2016), available at https://www.computereconomics.com/article.cfm?id=2185.

28 Case Study: A Confident Move to the Cloud for the University of Roehampton," available at https://www.civica.com/globalassets/7.document-downloads/2.uk-docs/case-studies/roehampton-case-study.pdf.

## BSA 관련 정보 /소프트웨어 협회

BSA/소프트웨어 협회(www.bsa.org)는 정부에 앞서 국제 시장에서의 국제 소프트웨어 산업을 주도하는 연합이다. 소속 회원들은 경제를 일으키고 현대적 삶을 개선시키는 소프트웨어 솔루션을 만드는 세계 최고의 혁신 업체들로 구성되었다.

워싱턴 DC에 본사를 두고 있고 60개국 이상의 국가에서 운영되고 있는 BSA는 합법적 소프트웨어의 사용를 촉진하는 준수 프로그램을 선도하고 디지털 경제에서 성장을 주도하며 기술적 혁신을 양성하는 공공 정책을 옹호한다.